Triangle PEERS
Research Triangle Park
North Carolina

29 June 2004

Dockets Management Branch (HFA-305)
Food and Drug Administration
5630 Fishers Lane, rm. 1061
Rockville, MD 20852

Re: Docket No. 2004N-0133

To Whom It May Concern:

Triangle PEERS is pleased to submit comments in response to the FDA's notice of public meeting and request for comments. Triangle PEERS (**P**art **E**leven **E**lectronic **R**ecords & **S**ignatures) is an association based in Research Triangle Park, North Carolina, whose members include representatives from over forty organizations, including pharmaceutical companies, clinical research organizations, academic research organizations, validation and IT systems consultants, and technology vendors. PEERS members possess expertise in a variety of perspectives such as technology, process engineering, quality assurance, regulatory affairs, data collection and management, legal, and data security. PEERS members focus primarily, although not exclusively, on the practical implementation of Part 11 in the conduct of clinical trials and how Part 11 may relate to Good Clinical Practices (GCPs).

General Background for PEERS Comments: Part 11 and the GCP Challenge

The FDA's Part 11 emphasis appears to have been focused on Good Manufacturing Practices (GMP) and Good Laboratory Practices (GLP). With both GMP and GLP, the regulations have clear record requirements and the regulations specify when signatures, initials, and other general signings are required. GMP and GLP regulations as a whole focus on overall record integrity. PEERS further recognizes that the GMP and GLP operations are more equipment intensive. The concept of automation of equipment is also less prevalent in GCP.

In comparison, the application of Part 11 to GCP records and respective systems is open to varying interpretation. Unlike GMP and GLP, the GCP regulations are less prescriptive regarding required records and signatures. The GCP regulations are based more on activities and responsibilities, giving rise to the issues of implied records. GCP systems are more related to data collection and storage, analysis and transformation. There is also frequent data movement

between systems, clinical investigational sites, laboratories, contract research organizations (CROs), and sponsors. From a GCP perspective, the challenge with Part 11 is its focus on record integrity for specific records required by the predicate regulations, yet in GCP the focus is on continued data integrity, because of conclusions that are reached, based on this data, for drug submissions/approvals. Data may be generated by a variety of sources, yet specific records *per se* may not be mentioned in the predicate regulations. As a result, the application of Part 11 to the GCP realm is challenging, leading to industry confusion and inconsistent interpretation.

Question A2: Should there be revisions/additions to the definitions in Part 11?

Yes. PEERS recommends that the following definitions be included in Section 11.3 of the regulation and referenced as appropriate in the regulation itself: "risk assessment," "risk management," "computer system validation," and "systems documentation."

Risk Assessment and Risk Management

PEERS is pleased that the FDA is advocating a risk-based approach for drugs and biologics, specifically stating in the *Part 11, Electronic Records; Electronic Signatures - Scope and Application* Guidance that the approach be based on a "justified and documented risk assessment." To date, however, risk topics have not been addressed in a way that allows them to be uniformly applied to all areas of the industry. In particular, those of us operating in the clinical IT arena find much of the existing information on risk to be of limited utility. The FDA's risk-based approach initially focused on the GMP community, and most references to external documents have continued to focus on manufacturing. The three recent draft FDA Guidances (*Premarketing Risk Assessment, Development and Use of Risk Minimization Action Plans, and Good Pharmacovigilance Practices and Pharmacoepidemiologic Assessment*) provide discussions of risk assessment, risk minimization, and risk management, but are targeted at the *product's* risks and benefits. Attempting to apply these concepts to electronic records and computer systems has not been addressed. In particular, the term "risk assessment" is frequently misinterpreted to mean "risk management."

The following suggested definitions incorporate elements of the *Premarketing Risk Assessment Guidance*, as well as the *NIST Risk Management Guide for Information Technology Systems*. The suggested definitions define the risk in terms of the concerns expressed by the FDA – impact to product quality, patient safety, and record integrity.

> **Risk Assessment:** The process of identifying and characterizing the nature, frequency, severity and impact of risks to product quality, patient safety, and record integrity. It includes analysis of safeguards that would mitigate this impact. Risk Assessment is the first step in the risk management process.

> **Risk Management**: The total, iterative process of identifying, controlling, and mitigating system risks. It includes risk assessment, benefit analysis, risk avoidance and mitigation, and monitoring effectiveness.

Computer System Validation

PEERS members agree that the computer system validation provision should be retained in Part 11, especially from the GCP perspective. In addition, defining computer system validation in Part 11 can provide a central, consistent definition. The predicate rules for GLP and GMP contain regulations that can be interpreted to cover computer systems validation; in contrast, GCP predicate rules do not mention computer systems, yet computer systems are used for key activities in clinical trials. Since computer system validation is not defined adequately in the predicate rules and can be interpreted in various ways, PEERS recommends that the definition for computer system validation be standardized, as proposed below. To avoid further confusion, PEERS also recommends that the major deliverables of validation – predetermined requirements, design specifications, testing against those requirements and specifications, and change control to maintain the computer system in a validated state – be listed with the definition.

> **Computer System Validation:** The ongoing process of establishing documented evidence that provides a high degree of assurance that a computerized system will consistently perform according to its predetermined requirements and quality attributes. This includes procedures, requirements and specifications, testing, and change control.

Systems Documentation

PEERS members believe that a definition is needed to clarify the scope of "systems documentation." The term "systems documentation" is often interpreted narrowly to mean only user manuals; others may consider "systems documentation" to include all computer system validation documentation deliverables plus the source code.

PEERS recommends the following definition be incorporated to provide consistent context and application for Section 11.10(k)(1) and (2):

> **Systems Documentation:** The collection of documents generated or compiled by the organization as evidence of validation planning and execution for computerized systems. This includes procedures, requirements and specifications, testing, change control, operation and maintenance documents, and associated reports.

Questions A3, B2 and D2: Is clarification needed regarding which records are required by predicate rules [especially when] those records are not specifically identified in GCP predicate rules?

Yes. PEERS requests that the FDA clarify what records are required by the GCP regulations (and hence Part 11 applies) and what records are implied because they meet an activity required by the regulations.

One of the largest challenges for the application of Part 11 to GCP is the issue of implied records. Confusion continues to exist within the industry, and particularly for those who focus on the GCP arena, about the issue of "implied" records – i.e., electronic records that are neither required to be kept by the Agency, nor required to be submitted, but that are kept in support of activities required by predicate rules.

As noted earlier, Part 11 applies more readily to the GMP and GLP regulations which are prescriptive and precise; GCP regulations lack explicit predicate rule record and signature requirements for required activities. As a result for GCP, there is a strong need for guidance on what records are specifically expected.

PEERS reiterates its earlier comments about implied records submitted to the FDA in response to the draft Guidance, *Scope and Application*:

> "Industry needs information from the FDA regarding Part 11 applicability where ostensible predicate rules exist but do not address or require specific records. Specifically, we ask for guidance where predicate rules require an activity but do not mention record requirements to demonstrate fulfillment of that activity. In such instances, is it an appropriate interpretation that electronic records maintained to prove that the activity occurred are not within the scope of predicate rules to trigger Part 11? For example, 21 CFR §312.50 and §312.56 require sponsors to monitor the progress of clinical investigations, yet no records are specifically mentioned [as evidence of this activity]. As a result, it would appear that monitoring visit reports retained electronically would not be subject to predicate rules with respect to Part 11."

Finally, PEERS requests clarification if globally applied standards such as *ICH Harmonised Tripartite Guidelines for Good Clinical Practice* are considered the equivalent of predicate rules.

Question B1. Should other areas of Part 11 incorporate the concept of risk-based approach?

Yes. PEERS recommends that a risk-based approach be adopted for open system security. The risk-based approach for open system security would address authenticity, integrity, and, as appropriate, confidentiality. PEERS further recommends that the FDA remove all references to specific technology in Section 11.30. By referencing certain technologies (digital signatures, encryption), the FDA has inadvertently limited what industry understands is acceptable for data transmission. Although the referenced technologies are recommendations not mandates, in practice alternative technologies are not being substituted for fear of lack of FDA acceptance. If specific current technology or approaches are desirable to demonstrate record integrity, these

are best mentioned in a Guidance, which can more easily be updated as technology changes.

Another recommended area for application of a risk-based approach includes the operational/sequence checks of Section 11.10(f). In some instances, the risks and consequences of performing steps and events out of order are low; therefore, the system need not be built to enforce the permitted sequencing.

QUESTION B1, Subpart B: Should we retain the validation provision under 11.10(b) required to ensure that a system meets predicate rule requirements for validation?

Yes. PEERS presumes that the FDA meant to reference Section 11.10(a) as the validation provision, instead of 11.10(b). For the reasons explained earlier in our comments to Question A.2, PEERS recommends that the validation provision be retained and further suggests that the term "validation" be clarified to reference "computer system validation."

Question B3: Should the requirements for electronic records submitted to FDA be separate from electronic records maintained to satisfy the predicate rule requirements?

Yes. PEERS members recommend distinguishing the requirements for submission of electronic records to the FDA from the issues surrounding the trustworthiness of the electronic records maintained to satisfy the predicate rules. The mechanism, acceptable electronic format, content requirements, etc., for submitting electronic records to the FDA are separate issues and should be defined elsewhere. However, the underlying controls to ensure the reliability and integrity of electronic records should be the same for both electronic records submitted to the FDA and electronic records maintained to satisfy predicate rule requirements.

Electronic records submitted to the FDA are used differently than electronic records used on-site, especially for clinical trials. For regulatory submissions, the FDA conducts reviews to assure safety, efficacy, and the scientific quality of clinical trials; the FDA does not directly conduct inspections of electronic records, electronic signatures, audit trails, etc. in submissions. An FDA review of a submission checks validity – rather than integrity – through cross-analysis (e.g., statistics). During on-site regulatory inspections, the FDA conducts inspections of the underlying electronic records, electronic signatures, audit trails, etc. against regulations to assure data integrity and security.

Question B4. Should Part 11 differentiate between open and closed systems?

Yes. PEERS recommends that the distinction between open and closed systems be maintained but a risk-based approach be adopted for open system security, as elaborated in our response to Question B1.

QUESTION C: Should Part 11 address investigations and follow-up when security breaches occur?

No. Investigation and follow-up are already implied in Sections 11.10(d) and 11.300(d). PEERS is opposed to the Part 11 regulation imposing additional regulatory burden; specifying how to investigate and follow-up constitutes unnecessary broadening of the scope of Part 11, as explained below.

Part 11 was written at a high level to allow for industry flexibility in implementing the regulation. Part 11 mandates the controls and safeguards to put in place without telling industry how to design, respond, or implement these measures. For example, Section 11.10(a) requires validation but the regulation does not specify the system lifecycle methodology to be used.

Industry practice and common sense necessitate investigation, root cause analysis, and corrective and preventive actions when security breaches or successive failed attempts occur. As a result, the regulation does not need to specify how industry must respond to security breaches; this is understood.

In PEERS' opinion, there is, however, a larger issue for the FDA to consider regarding the question of security. Does the FDA consider the security provisions in Section 11.300 applicable not only to electronic signatures but also to electronic records? PEERS members are divided as to whether the security provisions should explicitly extend to electronic records as well as electronic signatures. Those opposed are against scope creep and additional regulatory burden. Others consider application of the security provisions of Section 11.300 to be best practice.

The security controls identified in Section 11.300 are likely to be applied to the entire system if the system uses non-biometric electronic signature components - the user name and password security for basic user access and control (i.e., login). Because of the common occurrence of user name and password for login to systems that use non-biometric electronic signatures, some industry companies have applied the same security controls broadly across their systems. For those companies, this interpretation has come to be considered best practice and has subsequently become an expectation for achieving Part 11 compliance.

The alternative view is that while elements of the security provisions in Section 11.300 could, and in many instances should, be considered best practice, there is not a regulatory requirement to meet that particular standard. One of the main arguments here involves the requirements of Section 11.300(d) regarding

detection and reporting of attempted security breaches within the current context of electronic signatures only. If the Section 11.300 security provision were applied to all systems within scope of Part 11, detection and reporting of attempted security breaches would impose an additional burden, and in some cases, would be unattainable for instruments and/or equipment.

As a result, PEERS asks FDA to clarify the security provisions of Section 11.300 in its re-examination of the Part 11 regulation.

Question D8. Are there provisions of Part 11 that should be augmented, modified, or deleted as a result of new technologies that have become available since Part 11 was issued?

Yes. PEERS recommends that:

- the collaboration provision of Section 11.200(a) (3) be deleted since use of electronic signatures by the genuine owner is already addressed by Section 11.200(a) (2), and
- the concept of login as first signature be clarified.

Collaboration Provision

The collaboration provision of Section 11.200(a) (3) creates great industry and lay person confusion since it directly conflicts with the principle of signature usage only by the genuine owner. It has sometimes been interpreted to mean that it is acceptable to sign as someone else, provided that two people are involved. Clearly, use of another person's electronic signature should constitute fraud or falsification. PEERS further notes that most technologies –new and old – do not incorporate the collaboration concept into system design and functionality.

Login as First Signature

Industry has two very different interpretations of what constitutes the first electronic signature in a signing session. Unfortunately, this division of thought arises from conflicting statements between the preamble to the Part 11 regulation and the regulation itself.

Comment 124 to the Part 11 preamble, provides an example where "…an individual performs an initial system access or 'log on' which is effectively the first signing, by executing all components of the electronic signature (typically both an identification code and a password)." Some in industry have interpreted this comment to indicate that the FDA would accept system log on as the first electronic signature in a signing session.

However, Section 11.70 states, "Electronic signatures … shall be linked to their respective electronic records…." The alternative industry interpretation centers upon the fact that logging into the system does not constitute a first electronic signature because the user is not signing an underlying record; further, there is

no indication to the user that a signature is being applied so clear user intent as to the "meaning…associated with the signature" per 21 CFR 11.50(a)(3) is lacking. In essence, there is no electronic record and no meaning that can be associated with a login used as the first electronic signature in a signing session.

Without FDA clarification, industry will continue to be divided upon this point. New systems development, especially by vendors, must currently be tailored to specific company interpretations about log in as first signature. As a result, implementation of technological best standards is being hampered.

* * *

In conclusion, Triangle PEERS requests that the FDA revise the Part 11 regulation as discussed and/or provide guidance for the consistent application of Part 11 throughout the regulated industry, and more specifically in the GCP realm.

Sincerely,

Triangle PEERS
Research Triangle Park
North Carolina
http://peers.onsphere.com

REFERENCES

FDA, 21 CFR Part 11, Electronic Records, Electronic Signatures; Final Rule, Federal Register, Vol. 62, No. 54, 13429, March 20, 1997.

FDA, Guidance for Industry, *Part 11, Electronic Records; Electronic Signatures – Scope and Application*, August 2003.

FDA, Draft Guidance for Industry, *Development and Use of Risk Minimization Action Plans*, May 2004.

FDA, Draft Guidance for Industry, *Good Pharmacovigilance Practices and Pharmacoepidemiologic Assessment*, May 2004.

FDA Draft Guidance for Industry, *Premarketing Risk Assessment*, May 2004

United States Department of Commerce, National Institute of Standards and Technology (NIST), *Risk Management Guide for Information Technology Systems*, Special Publication 800-30, October 2001.